IN THE CLAIMS:

1-12. (canceled)

13. (currently amended) A method of authenticating the identity of a user to determine access to a system, comprising:

providing a possession-based data instance, a modified version of the possession-based data instance, a knowledge-based data instance, a biometric-based data instance, and a modified version of the biometric-based data instance;

generating a first cryptographic key based on the knowledge-based data instance;

applying the first cryptographic key to the modified version of the possession-based data instance to generate a first recovered data instance;

interrogating the first recovered data instance against the possession-based data instance to generate a possession value as a result of a first correspondence evaluation;

applying the first cryptographic key to the modified version of the biometric-based data instance to generate a second recovered data instance;

interrogating the second recovered data instance against the biometric-based data instance to generate a biometric value as a result of a second correspondence evaluation;

combining the first cryptographic key, the possession value, and the biometric value to form a second cryptographic key;

restricting the user's access to the system if the user's identity is not authenticated, based at least in part on the ~~authentication value~~ second cryptographic key; and

granting the user's access to the system if the user's identity is authenticated, based at least in part on the ~~authentication value~~ second cryptographic key.

14. (original) The method of claim 13, wherein restricting the user's access includes denying the user's access.

15. (original) The method of claim 13, wherein the modified version of the biometric-based data instance is a first modified version of the biometric-based data instance, and the biometric value is a second modified version of the biometric-based data instance.

16. (original) The method of claim 15, wherein the biometric value is a cryptographic hash of the biometric-based data instance.

17. (currently amended) The method of claim 13, wherein restricting the user's access to the system and granting the user's access to the system is based on a modified version of the second ~~crytogrphic~~ cryptographic key.

18. (previously submitted) The method of claim 17, wherein the modified version of the second cryptographic key is a cryptographic hash of the second cryptographic key.

19-24. (canceled)

25. (previously submitted) A method of authenticating the identity of a user to determine access to a system, comprising:

providing a possession-based data instance, a biometric-based data instance, and a modified version of the biometric-based data instance;

applying the possession-based data instance to the modified version of the biometric-based data instance to generate a recovered data instance;

interrogating the recovered data instance against the biometric-based data instance to generate a biometric value as a result of a correspondence evaluation;

combining the possession-based data instance and the biometric value to form a cryptographic key;

evaluating the cryptographic key to determine if the user's identity is authenticated;

restricting the user's access to the system if the user's identity is not authenticated, based at least in part on the cryptographic key; and

granting the user's access to the system if the user's identity is authenticated, based at least in part on the cryptographic key.

26. (original) The method of claim 25, wherein restricting the user's access includes denying the user's access.

27. (original) The method of claim 25, wherein the modified version of the biometric-based data instance is a first modified version of the biometric-based data

instance, and the biometric value is a second modified version of the biometric-based data instance.

28. (original) The method of claim 27, wherein the biometric value is a cryptographic hash of the biometric-based data instance.

29. (previously submitted) The method of claim 25, wherein restricting the user's access to the system and granting the user's access to the system is based on a modified version of the cryptographic key.

30. (previously submitted) The method of claim 29, wherein the modified version of the cryptographic key is a cryptographic hash of the cryptographic key.